



UNITED STATES PATENT AND TRADEMARK OFFICE

[Handwritten signature]

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,853	01/31/2002	James Kleinsteinber	112-0019US	1224

29855 7590 08/15/2006

WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI,
L.L.P.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT PAPER NUMBER

2134

DATE MAILED: 08/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/062,853

Applicant(s)

KLEINSTEIBER ET AL.

Examiner

Christopher J. Brown

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-53 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-53 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2/21/06, 4/27/06
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 5/01/2006 have been fully considered but they are not persuasive.

Applicant argues with regards to the motivation of the combination of Li US 5,473,599 with Daley "Entity Authentication using Public Key Cryptography".

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one

Art Unit: 2134

of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation is found in knowledge generally available to one of ordinary skill in the art.

In response to applicant's argument that Li teaches away from security, the examiner argues that to teach away the reference in question must specifically state that security is unwanted or cannot happen. Li does not state that security is unwanted, and in fact uses a very weak security protocol.

In the applicant's argument that there can be no reasonable expectation of success, the applicant argues that the security of Daley would "change the principle operation of Li changing it from a system and method for increasing reliability through redundant routers to a system for increasing security". The examiner argues that although Daley is adding heightened security to Li, it in no way is "changing the principle operation". The combination of the two references merely enhances the security of Li with the security of Daley.

Applicant argues that Li does not teach derivatives or comparing derivatives with secret information. The applicant is correct in that Li does not teach derivatives or secret information. The examiner has not cited Li, and instead relies on Daley to teach such limitations.

Art Unit: 2134

Applicant argues that Daley does not teach comparison derivatives or comparing derivatives with secret facts. The examiner admits in the office action that Daley does not explicitly state the verification method used, but that Daley does teach verification of derivatives. The examiner took official notice and incorporated “Applied Cryptography” by Bruce Schneier which indicates that a digital signature is compared to the received secret data (or a new hash generated of said secret data) as a means of validation. Thus, Daley with the official notice taken by the examiner, does teach comparison of derivatives and secret facts.

Applicant’s argument with respect tot the Oath is not persuasive. The examiner has not objected to the oath because of a missing joint inventor who refuses to join the application for a patent. The examiner cannot find the stated items, for *any* inventor for the application. Appropriate Correction is required.

Applicant’s arguments, see with respect to USC 112 rejections have been fully considered and are persuasive. The USC 112 rejections have been withdrawn.

The rejection below is substantially similar to the previous office action.

Claim Objections

Art Unit: 2134

2. Claims 24, 25, 26, 29, 31, 34, are objected to because of the following informalities: The claims are dependent on claim 22, it appears that they should be dependent on claim 23. Appropriate correction is required.

Claims 38, 39, 40, 43, 47 are objected to because of the following informalities: The claims are dependent on claim 35, it appears that they should be dependent on claim 37. Appropriate correction is required.

Claims 52, and 53 are objected to because of the following informalities: The claims are dependent on claim 49, it appears that they should be dependent on claim 51. Appropriate correction is required.

Oath/Declaration

3. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

It does not state that the person making the oath or declaration believes the named inventor or inventors to be the original and first inventor or inventors of the subject matter which is claimed and for which a patent is sought.

Art Unit: 2134

It does not identify the mailing address of each inventor. A mailing address is an address at which an inventor customarily receives his or her mail and may be either a home or business address. The mailing address should include the ZIP Code designation. The mailing address may be provided in an application data sheet or a supplemental oath or declaration. See 37 CFR 1.63(c) and 37 CFR 1.76.

It does not state that the person making the oath or declaration has reviewed and understands the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration.

It does not identify the citizenship of each inventor.

It does not identify the city and either state or foreign country of residence of each inventor. The residence information may be provided on either an application data sheet or supplemental oath or declaration.

It does not state that the person making the oath or declaration acknowledges the duty to disclose to the Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

The clause regarding "willful false statements ..." required by 37 CFR 1.68 has been omitted.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1-19, 21-32, 34-53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Li US 5,473,599 in view of "Entity Authentication using public key cryptography" William Daley

Art Unit: 2134

As per claim 1, Li teaches a system of routers that communicate through hello messages and include authentication messages, (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16). Li does not teach a strong authentication system.

Daley teaches a strong authentication protocol comprising: sending a secret fact (random nonce) from sender B to a receiver A, (page 21, 23). Daley states receiving a second type derivative (signature of A) of said first secret fact, pre-defined information (certificate of A with key information). Daley teaches that receiver B verifies second type derivative and secret fact, (page 23). Daley teaches that receiver B verifies the certificate or chain of certificates (page 23).

Although Daley does not explicitly state the method of verification of the signature, the examiner takes official notice that it is well known in the art, (Applied Cryptography Schneier pg 38-39). Daley does not teach the method of certificate verification the examiner takes official notice that this is well known in the art, and that the issuing certificate authority signs the certificate creating a third type derivative (Applied Cryptography Schneier pg 574-576).

It would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

As per claim 2, Li teaches the routers use the same protocols, which use the same ports, (Col 8 lines 4-7).

As per claims 3, and 4, Daley teaches verifying the digital signature, which includes reversing (decryption) and creating (hashing).

As per claim 5, Daley teaches that second type derivative is associated with second switch (A) (page 23).

As per claim 6, Daley teaches a certificate or chain of certificates issued by a certificate authority (page 23). Daley teaches validation of said certificate. The examiner takes official notice that validation includes a certificate authority trusted by both parties in the authentication.

As per claim 7, Daley teaches pre-defined information is a certificate that includes encryption key information, (pg 23).

As per claims 8, 9, 24, 25, 38, 39, and 52 Daley teaches sending a one time random number as a first secret fact, (pg 22).

As per claims 10, 23, 37, 50, and 51 Li teaches a system of routers that communicate through hello messages and include authentication messages, (Col 3 lines 1-4, Col 10 line 65-Col 11 line 16). Li does not teach a strong authentication system.

Daley teaches a strong authentication protocol comprising: sending a secret fact (random nonce B) from sender B to a receiver A, (page 21, 23). Daley states receiving a second type derivative (signature of A) of said first fact, pre-defined information (certificate of A with key information), and second fact (random nonce A). Daley teaches that B creates a first-type derivative (signature of B) of said second fact, and sends it to A, (page 24). Daley teaches B sending first-type

Art Unit: 2134

derivative, defined information (certificate of B with key information, and third type derivative), to A(pg 21, 24. Daley teaches A verifies first type derivative, and B verifies second type derivative. Daley teaches both A and B verify the third type derivative. . Daley teaches that A and B verify the certificate or chain of certificates (page 23-25).

Although Daley does not explicitly state the method of verification of the signature, the examiner takes official notice that it is well known in the art, (Applied Cryptography Schneier pg 38-39). Daley does not teach the method of certificate verification the examiner takes official notice that this is well known in the art, and that the issuing certificate authority signs the certificate creating a third type derivative (Applied Cryptography Schneier pg 574-576).

It would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

As per claim 11, Daley teaches verifying the digital signature, which includes reversing (decryption) and comparing.

As per claim 12, Daley teaches verifying the signature which includes creating (hashing) and comparing.

As per claims 13, 14, 15, 26, 27, 28, 40, 41, and 42, Daley teaches creating a second type derivative by creating a signature of a first fact. Schneier provides

Art Unit: 2134

the method of creating a signature which is well known in the art. The method of which includes hashing the first fact and encrypting said hash with a private key, (Schneier pg 38-39).

As per claims 16, 29, and 43, Daley teaches defined information is a certificate that includes encryption key information, (pg 23).

As per claims 17, 30, and 44, Daley teaches defined information is a certificate. Schneier provides the well known structure of the certificate which includes a public key, (pg 574).

As per claims 18, 31, and 45 Daley teaches a certificate or chain of certificates issued by a certificate authority (page 23). Daley teaches validation of said certificate. The examiner takes official notice that validation includes a certificate authority trusted by both parties in the authentication.

As per claims 19, 32, and 46 Daley teaches a certificate or chain of certificates issued by a certificate authority (page 23). Daley teaches validation of said certificate. The examiner takes official notice that validation includes a certificate authority trusted by both parties in the authentication. Schneier provides the well known method of verification which includes using a public key to check the signature created by the private key of the certificate authority, (pg 574-576).

As per claims 21, 22, 34, 35, 36, 47, 48, and 49 Daley teaches validation of the defined information The examiner takes official notice that this is well known in

the art, and that the issuing certificate authority signs the certificate creating a third type derivative, and in verification the private key signature is reversed (decrypted) and compared, (Applied Cryptography Schneier pg 574-576).

As per claim 53, Li teaches priority levels of the routers determine status (Col 2 lines 44-53).

Claims 20, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Li US 5,473,599 in view of "Entity Authentication using public key cryptography" William Daley in view of JP02001148697A

As per claims 20 and 33, Daley teaches that receiver B verifies the certificate or chain of certificates (page 23).

Daley does not teach the method of certificate verification the examiner takes official notice that this is well known in the art, and that the issuing certificate authority signs the certificate creating a third type derivative (Applied Cryptography Schneier pg 574-576).

It would have been obvious to one of ordinary skill in the art to use the authentication system of Daley with the routers of Li, because the strong authentication would enhance the security of the routers.

Neither Daley or Li teach that the authority is the manufacturer of the device. JP02001148687 teaches a manufacturer stores a certificate and manufacturer signature made by a private key on each device. (Abstract).

Art Unit: 2134

It would have been obvious to one of ordinary skill in the art to use the method of JP02001148697 because it allows every device to communicate safely over a channel with low reliability.

Conclusion

5. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jaques Louis Jaques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown

8/8/06

Jacques Louis Jacques
JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100